

AO 106 (Rev. 04/10) Application for a Search Warrant

United States District Court  
for the  
Western District of New York



In the Matter of the Search of

*(Briefly describe the property to be searched or identify the person by name and address.)*

82 Culver Rd, Upper, Buffalo, New York 14220

Case No. 20-mj- 5282

**APPLICATION FOR A SEARCH WARRANT**

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

82 Culver Rd, Upper, Buffalo, New York 14220, which is more fully described in Attachment A, which is attached hereto and incorporated by reference herein

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated by reference herein.

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

\_\_\_\_\_  
*Applicant's signature*

KATHRYN M. GAMBLE  
SPECIAL AGENT  
HOMELAND SECURITY INVESTIGATIONS  
\_\_\_\_\_  
*Printed name and title*

Sworn to telephonically.

Date: October 30, 2020

\_\_\_\_\_  
*Judge's signature*

City and state: Buffalo, New York

HONORABLE MICHAEL J. ROEMER  
UNITED STATES MAGISTRATE JUDGE  
\_\_\_\_\_  
*Printed name and Title*

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT APPLICATION**

I, Kathryn M. Gamble, being duly sworn, depose and state the following:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI). I have been employed as a Special Agent since June 2008. I am currently assigned to the Buffalo, New York office. I am responsible for investigating crimes involving child exploitation and child pornography including violations of Title 18, United States Code, Sections 2251(a) (production of child pornography); 2422(b) (online enticement of minors); 2252A(a)(2)(A) (receipt of child pornography); and 2252A(a)(5)(B) (possession of child pornography). I have received extensive training with respect to child exploitation and child pornography investigations. I have participated in hundreds of child exploitation and child pornography investigations and executed numerous search warrants involving child pornography and the seizure of computers and other storage media. I have interviewed many individuals involved in child pornography and the sexual exploitation of children and have viewed several thousand of images and videos depicting child pornography as defined by Title 18, United States Code, Section 2256(8).

2. This affidavit is submitted in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the property located at 82 Culver Rd, Upper, Buffalo, NY 14220 (hereinafter the "SUBJECT PREMISES") and the content of electronic storage devices located therein. The SUBJECT PREMISES is more particularly described in Attachment A of this affidavit.

3. As set forth in more detail below, there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251(a) (production of child pornography), 2252A(a)(2)(A) (receipt of child pornography), and 2252A(a)(5)(B) (possession of child pornography) are located within the SUBJECT PREMISES. The items to be seized are more particularly described in Attachment B of this affidavit.

4. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES.

#### **DEFINITIONS**

5. The following definitions apply to this affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image,

computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. “Computer,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, other mobile devices, desktop computers, notebook computers, tablets, server computers, and network hardware. See 18 U.S.C. § 1030(e)(1).

d. “Computer hardware,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. “Computer passwords and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software,

documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

f. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

g. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

h. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

i. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web

hosting, email, remote storage, and co-location of computers and other communications equipment.

j. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

k. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

m. “Mobile application” or “chat application,” as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

n. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. “Remote computing service”, as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

p. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

q. A “storage medium” is any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

r. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

s. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short



in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

**PROBABLE CAUSE**

6. On or about April 22, 2020, a detective in Los Angeles County, California received information relating to a complaint made by a 9-year-old minor female (hereinafter, MV1). MV1 reported that she had been contacted by an unknown male individual through a social media application called LiveMe. LiveMe is an application that allows its users to live stream to other LiveMe users what they are doing at any given time. LiveMe users who are watching live stream videos, can comment on the videos and the broadcasters can engage their viewers in chat communication. It is accessible by using a cell phone, tablet, or desktop computer.

7. MV1 indicated she had created the LiveMe account using her mother's email address. Shortly after creating the account, she began to live stream herself playing with some of her toys. MV1 was contacted by a LiveMe user by the name "HAZMETUYA" (hereinafter, "the TARGET"), which loosely translated from Spanish into English means "Make me yours." The TARGET provided MV1 his cell phone number, (716) 394-7580, and suggested they began communicating with each other through cell phone text messaging.

8. MV1 and the TARGET began text messaging each other on or about March 27, 2020. The TARGET asked MV1 to send him a picture of her genitals; MV1 sent one picture. The TARGET responded by sending MV1 two pictures of his penis and a video of himself exposing his penis. The TARGET then asked MV1 to open her legs and show more of her genitals.



9. MV1's mother discovered the text messages on her daughter's cell phone after taking it away from her as punishment. MV1's mother went through the cell phone and she discovered the application LiveMe and tried to access it. She was not able to access the application using the myriad of possible password combinations MV1 may have used, but she did discover that the account had been banned for violating platform rules. MV1's mother was able to obtain a screenshot of the notification. The screenshot contained MV1's username, user identification and specific rules she had violated: Adult Content, No bloodiness and violence, No usage by the underage, No malicious content. There were also three photographs of MV1's face which clearly depicted she was a minor. According to the company's General Terms & Conditions-User Eligibility: "The Service is restricted for use by any persons under the age of 18."

10. The Los Angeles County detective was able to view and preserve text message communication between MV1 and the TARGET with phone number (716) 394-7580. The detective observed the three (3) sexually explicit files sent by the TARGET to MV1, namely, files depicting an adult male erect penis. The detective also observed two (2) sexually explicit files sent by MV1 to the TARGET, that depict her genitals. The detective observed some chat conversation between MV1 and the TARGET, wherein the TARGET tells MV1 to, "Open you legs very well" and "open you delicious pussy very very well".

11. On April 24, 2020, the Los Angeles County detective applied for and received search warrants for the TARGET Verizon cell phone account information and MV1's LiveMe account information. The warrants were signed by Honorable Craig Veals, Judge of the Superior Court of California, County of Los Angeles.

12. On May 5, 2020, Verizon provided a return to the warrant. The subscriber information associated to cell phone number (716) 394-7580 showed that the account was registered to Kathleen Reeb-Reascos at 82 Culver Road, Buffalo, NY 14220. The IMEI associated to this account was provided as 353057102867259. Utilizing this information, the Los Angeles County detective was able to apply for and receive a California state search warrant for the TARGET LiveMe account.

13. On May 13, 2020, LiveMe America provided a return to the warrant for MV1's account. The return showed the chat communications that occurred between the TARGET and MV1.

14. Your affiant reviewed the LiveMe chats that occurred between the TARGET and MV1. Within the chat communication, MV1 provides her age as 12 years old; the TARGET states that he is 16 years old. The TARGET tells MV1 that she looks closer to 14 years old. The TARGET tells MV1 that he is horny and "I'm hard" and asks MV1 if that is okay. The TARGET provides his name as "nick" and again tells MV1 that he is "very very hard". The TARGET tells MV1 that she looks great and "you sexys wet lips make me super super hard", "I like you", "More wet lips I'm more and more hard". The TARGET continues to make sexual comments, and MV1 replies, "I'm 12 and you are 16". The TARGET continues on in the same manner, "You make my dck more big", "I'm imagine licking you cute pusy right now", "Open you imagination my gorgeous and sexy princess", "I'm imagine my tongue between you legs licking you delicious pusy". The TARGET asks MV1 for sexually explicit pictures, "Show you cute pusy", "You pusy plzz", and tells her how to masturbate, "Used 2 fingers very fast up and down". MV1 finally tells the TARGET, "I'll send you a picture". The TARGET and MV1 then exchange phone numbers.

15. Your affiant reviewed the subsequent text message communication that occurred between MV1 and the TARGET using telephone number (716) 394-7580. This conversation starts out with the TARGET saying to MV1, "Let me see". MV1 then sends one picture depicting a close up view of a prepubescent vagina. The stomach of the child is also exposed and a gray tshirt with a character on it can be seen covering part of the child's chest. The TARGET responds, "Open your legs very well", "Plzzz". The TARGET then sends multiple pictures depicting an erect, adult male penis. MV1 sends the TARGET one more picture depicting a prepubescent vagina. The child is still wearing the gray tshirt and the character on the shirt appears to be a raccoon. The TARGET response was, "Open you delicious pussy very very well".

16. On May 13, 2020, LiveMe America also provided a return for the TARGET's LiveMe account. The account was created on March 21, 2020. The account username, "HAZEMETYUYA" was changed to "Lovewet". Some other subscriber information included:

UID:	1241105450347405313
SID:	197178268
Username:	Lovewet <del>✖</del> □
Registration Date:	2020-3-21 04:52:52
Common IP Addresses:	174.224.143.188 - Verizon 174.224.133.214 - Verizon 45.46.170.24 – Charter Communications
Device Model:	iPhone 11, 8

17. In addition to the subscriber information, Your affiant was able to view the chat communication that the TARGET engaged in with MV1. Your affiant also observed chat communication that the TARGET engaged in with other LiveMe users. The TARGET was

communicating with multiple LiveMe users who provide their ages as 11 and 13 years old. All of the language/chat communication that the TARGET used is sexual in nature. For example, the TARGET language used with other users includes, "Make you cute pussy very wet", "Play with you cute kitty right now", "You're gorgeous and sexy girl. You like dance or gymnastics", "Try and make cute pussy very wet", "Let me see you legs. Make me more hard my beautiful princess", "You have brush electric"". Many users expressed disinterest and disapproval of the TARGET's requests. One user tells the TARGET, "No ur a perv u child predator" and another user tells him, "Don't talk to me any more I will get you banned". Other users told the TARGET that they were going to block him and one user stated that they were going to call the police. This chat content that was provided by LiveMe includes the TARGET chat history from March 22, 2020 through April 24, 2020.

18. On May 20, 2020, the Los Angeles County Detective applied for and received a California state search warrant for the TARGET's IP address, 45.46.170.24, which was registered to Charter Communications.

19. On June 10, 2020, Charter Communications provided a return to the search warrant showing the account subscriber information as Kathleen Reeb Reascos, 82 Culver Road, UPPR, Buffalo, NY 14220.

20. On October 19, 2020, HSI Buffalo agents requested a mail check to confirm who is receiving mail at 82 Culver Rd., Buffalo, NY 14220. The information returned showed that individuals with the surname "Reeb-Reascos" receive mail at this address.

21. On October 28, 2020, your affiant utilized a publicly available website to query “82 Culver Rd., Buffalo, NY” and discovered that the residents are listed as Kathleen Reeb (DOB: 09/24/1984) and Segundo Nicanor REASCOS-RODRIGUEZ (DOB: 10/05/1980). This website also lists the property as a multi-family residence.

22. On October 28, 2020, your affiant obtained New York Department of Motor Vehicle (DMV) license information for S N, REASCOS RODRIGUEZ (DOB: 10/05/1980) that lists his address as 82 Culver Rd. UPPR, Buffalo, NY 14220. Your affiant also obtained DMV records for vehicles registered to REASCOS RODRIGUEZ and discovered that he is the registered owner of a Chevrolet Equinox bearing NY/HDU1392.

23. On October 28, 2020, Your affiant conducted surveillance at 82 Culver Rd., Buffalo, NY 14220 and observed a dark gray Chevrolet Equinox bearing NY/HDU1392 parked in the driveway of the residence.

24. HSI Buffalo agents checked with utility providers and were advised that there are only two subscribers with accounts at 82 Culver Rd., Buffalo, NY 14220.

#### **BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET**

25. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones and/or mobile phones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be



automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO PRODUCE, ADVERTISE,  
TRANSPORT, DISTRIBUTE, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT  
TO VIEW CHILD PORNOGRAPHY**

26. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, and/or possess child pornography:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography

distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if an individual uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in the individual's home, the SUBJECT PREMISES, as set forth in Attachment A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

### **CONCLUSION**

27. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the location described in Attachment A. I respectfully request that this Court issue a search warrant for the location described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

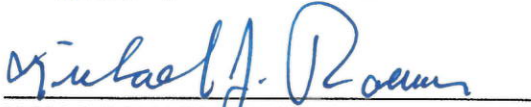
28. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital

evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



KATHRYN M. GAMBLE  
Special Agent  
Homeland Security Investigations

Sworn to telephonically  
this 20<sup>th</sup> day of October, 2020



HON. MICHAEL J. ROEMER  
United States Magistrate Judge

**ATTACHMENT A**

**DESCRIPTION OF LOCATION TO BE SEARCHED**

The property located at 82 Culver Rd, Upper, Buffalo, NY 14220 (the "SUBJECT PREMISES"). The SUBJECT PREMISES, as depicted below, is a two story, multi-family home, beige in color with red shutters. The numbers "82" are clearly depicted next to the front door. The SUBJECT PREMISES includes only the Upper Unit of this residence.



**ATTACHMENT B**

**ITEMS TO BE SEARCHED FOR AND SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely, violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2)(A), and 2252A(a)(5)(B):

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;

- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;
- e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. contextual information necessary to understand the evidence described in this attachment.



3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography, as defined in 18 U.S.C. § 2256(8), and child erotica.
5. Communications relating to the production, receipt, or possession of child pornography.
6. Records, information, and items relating to violations of the statutes described above including:
  - a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;
  - b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
  - c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, and includes smartphones, other mobile phones, other mobile

devices, desktop computers, notebook computers, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.